DIE HAUSORDNUNG FÜR IT-SYSTEME

CHECKLISTE: NIS-2 EINFACH ERKLÄRT

01. Juni 2024

NIS-2 sorgt in vielen Köpfen für Unsicherheit. Dabei lässt sie sich gut mit der Hausordnung, wie sie in Mehrfamilienhäusern oder Firmengebäuden existiert, vergleichen: Die europaweite Direktive ist das Regelwerk (Hausordnung), deren Einhaltung Dienstleister (analog zum Hausmeister) für Unternehmen (quasi die Bewohner:innen) sicherstellen. Doch was ist neu an NIS-2? Welche Maßnahmen müssen Firmen implementieren? Die nachfolgende Checkliste bringt es leicht verständlich auf den Punkt.

Nur wenige Anforderungen von NIS-2 sind grundlegend neu.
Zu den Neuerungen gehört vor allem zweierlei:

1. Ab Mitte Oktober 2024 müssen Unternehmen relevante Security-Vorfälle melden. Sind sie dazu nicht in der Lage oder lassen sie die Meldefrist verstreichen, drohen empfindliche Bußgelder.
2. Davon unberührt führt NIS-2 auch viele Einzelmaßnahmen, die Firmen bereits umsetzen, in ein Regelwerk zusammen.

Dennoch ergeben sich für Unternehmen zentrale Aspekte, welche die NIS-2 betont und auf die Unternehmen besonders achten sollten.

1. System-Inventur

Unternehmen müssen ihre Systeme vollständig inventarisieren und Assets professionell managen. Nur so können sie Cyber-Risiken verlässlich handhaben. Doch kennen Firmen ihre Unternehmenswerte? Und sind diese vor Missbrauch oder Diebstahl geschützt? In der Haus-Analogie gedacht: Wie oft verstaut die Mieterschaft Schätze auf dem Dachboden und verliert gänzlich den Überblick darüber, was sie eigentlich alles Wertvolles besitzt. Vergleichbar dazu ist womöglich der Quellcode einer geschäftskritischen Unternehmens-Software auf einem Speichergerät unterhalb eines Schreibtisches abgelegt – und damit vor unberechtigten Zugriffen nicht sicher. Eine umfassende Bestandsaufnahme ist also der erste Schritt.

2. System-Monitoring

Unternehmen müssen ihre Systeme auf Schwachstellen scannen und ein Vorgehen für deren Beseitigung definieren. Fakt ist: Unternehmen werden früher oder später Opfer eines Cyber-Angriffs. Sie benötigen darum zwingend Systeme zur Angriffserkennung (SzA). Nur so können sie einen drohenden Angriff frühzeitig erkennen und angemessen darauf reagieren. Zudem braucht es weitere Maßnahmen wie Pentesting, Security Audits, Log Monitoring und Compliance Monitoring. Vergleichbar ist diese Anforderung mit der notwendigen Installation von Rauchmeldern im Haus, die eine Art Frühwarnsystem darstellen – wenn auch nicht ohne Restrisiko. Die Batterie könnte leer oder der Rauchmelder defekt sein. Für Unternehmen heißt dies, dass trotz ergriffener Prevention- und Detection-Maßnahmen ein Hacker-Angriff unbemerkt bleiben kann.

3. Schadenserkennung

Unternehmen müssen Schwachstellen identifizieren, bewerten, priorisieren und beheben. Darum sind automatisierte Detection- und Response-Maßnahmen ebenso in den Kernprozessen von Unternehmen zu verankern wie das Patch Management. Ein typisches Problem: Ein Unternehmen mit komplexer IT-Systemlandschaft setzt für das Schwachstellenmanagement auf lokale Excel-Listen. Weil es aufgrund der Menge an Schwachstellen den Überblick verliert, dringen Hacker in die Unternehmens-IT ein. Zum Verständnis der Vergleich: Ist im Haus beispielsweise eine Fensterscheibe oder ein Schloss defekt, lässt sich dies leicht erkennen und beheben. Doch was, wenn in einem Gebäudekomplex gleich mehrere solcher Schwachstellen identifiziert werden? Dann gilt es, die Dringlichkeit der Reparaturmaßnahmen zu bewerten und verschiedene Handwerker bei der Schadensbehebung zu koordinieren.

4. Sensibilisierung

Unternehmen benötigen zentrale Richtlinien und müssen Mitarbeitende und Geschäftsführung für die allgegenwärtigen Cyber-Gefahren sensibilisieren. Zudem ist neben Identity und Access Management auch Incident Management Pflicht. Man stelle sich nur vor: Weil Mitarbeitende unsichere Passwörter verwenden, sind ihre E-Mail-Konten in der Cloud nicht gesichert. Zugleich dürfen sie auf Geschäfts-Software zugreifen, ohne sich mit einem zweiten Faktor zu authentifizieren. Ein Krimineller dringt dann über gehackte E-Mail-Konten in die Unternehmens-IT ein und breitet sich immer weiter aus. Sensibilisierung ist unverzichtbar, aber Richtlinien verankern diese verbindlich für alle Beteiligten: So findet man eben auch in Hausordnungen Vorgaben, die es beispielsweise untersagen, bei Unbekannten den Haustüröffner zu betätigen oder für Paketdienste Ablageorte innerhalb der Mieteinrichtung zu vereinbaren. Für die Unternehmens-IT bedeutet das: Mitarbeitende müssen den Umgang mit sensiblen Daten beherrschen. Es braucht Regeln für den Zugriff auf diese Daten. Und es muss überprüfbar sein, ob sie fehlerhaft sind.

5. Transparenz

Unternehmen müssen ihre Systeme mithilfe von Tools für Endpoint Detection and Response (EDR), Network Detection and Response (NDR) sowie Security Information and Event Management (SIEM) fortlaufend überwachen und bezüglich ihrer Sicherheitsrisiken bewerten. Das Problem: Unternehmen wissen häufig nicht, welche Systeme ihre Mitarbeitenden einsetzen. Diese unbekannten oder „vergessenen“ Tools sind im Scope nicht erfasst und werden darum weder auf Schwachstellen gescannt noch gepatcht. Daneben entstehen ungewollte Abhängigkeiten, weil das Personal unautorisierte Systeme nutzt, um wichtige Prozesse zu managen. Im Treppenhaus kann beispielsweise ein unbedarft abgelegter Müllsack ein hohes Brandrisiko für alle Bewohner:innen darstellen, welches sich so auch nicht auf einen Blick abschätzen lässt.

6. Notfallpläne

Unternehmen müssen mit vorab definierten Response-Maßnahmen im Angriffsfall unmittelbar reagieren können. Sie sind dazu verpflichtet, sicherheitsrelevante Vorfälle in einem bestimmten Zeitfenster zu melden – einschließlich Zwischen- und Abschlussmeldungen. Diese Meldewege müssen vorbereitet, bekannt und implementiert sein. Sensible Assets gilt es speziell abzusichern. Zudem müssen Unternehmen belastbare Vorkehrungen für Notfälle und bestimmte Szenarien treffen: Notfallplanung, Notfallmanagement und Pläne für die Wiederherstellung des Geschäftsbetriebs sind Pflicht. So ist beispielsweise auszuschließen, dass hochsensible Daten auf mobilen Geräten der Mitarbeitenden existieren, sodass unbefugte Dritte bei Verlust oder Diebstahl bequem Zugang zu den Daten erhalten und das Unternehmen so Opfer von Hackerangriffen oder Erpressungen wird. Jeder kennt es: In Mehrfamilienhäusern und Firmengebäuden müssen alle Fluchtwege ausgewiesen, gekennzeichnet und stets ungehindert zugänglich sein. Auch der Verlust von Zentralschlüsseln ist immer direkt anzuzeigen.

7. Kommunikationswege

Es sind Verhaltensanweisungen für das Personal vorzubereiten und zu kommunizieren. Über Änderungen ist jederzeit zur informieren. Interaktive (Online-)Schulungen dienen dem Zweck, die Belegschaft zu trainieren und ihr Wissen regelmäßig aufzufrischen. Während es von der Hausverwaltung meist Aushänge, Briefe oder E-Mails mit wichtigen Handlungsanweisungen gibt, gilt für IT-Sicherheit in Unternehmen: Es braucht abgestimmte Kommunikations- und Notfallpläne, die allen zugänglich sind. Zudem sind notwendige Änderungen sorgfältig vorzubereiten, zu bewerten, mit risikominimierenden Maßnahmen zu unterlegen und zu dokumentieren. Und natürlich müssen sich im Notfall alle entsprechend verhalten. Hat ein Security-Dienstleister für ein Unternehmen belastbare Notfallpläne ausgearbeitet, doch die Firma bespricht diese Strategien nicht mit dem Personal, kommt es bei einer Cyber-Attacke schnell zu Panik oder unbedachten Handlungen, die das Problem unter Umständen verschärfen. Man denke nur daran, was passiert, wenn die Bewohner:innen eines Mietshauses nicht über die geplante Instandhaltung der Wasserleitungen mit Abschaltung aller Leitungen informiert werden.

8. Supply-Chain-Risiken

Es gilt, Supply-Chain-Risiken ganzheitlich abzufragen und wirkungsvoll zu managen. Hierfür sollten Unternehmen auf branchenspezifische, bewährte Best Practices setzen. Für Geschäftsgebäude wie für die Unternehmenssysteme gilt: Lieferanten, Partner und andere Betriebsfremde, die Zugang haben oder auf Applikationen zugreifen, sind ins

Risikomanagement zu integrieren. Im Bereich IT sind zum einen nur gesicherte IT-Lösungen bereitzustellen, zum anderen ist zu gewährleisten, dass Externe selbst nicht zum Sicherheitsrisiko werden. Darum sind Zero Trust und Multi-Faktor-Authentifizierung unverzichtbar.

Fazit

Vor dem Hintergrund dieser acht Handlungsfelder müssen Unternehmen

- rechtssicher beurteilen, inwieweit sie von den NIS-2-Vorgaben betroffen sind,
- sich einen Überblick verschaffen, welche Maßnahmen bereits umgesetzt sind,
- die Umsetzung der Maßnahmen konsequent priorisieren,
- die damit verbundenen finanziellen und personellen Aufwendungen bestimmen,
- die Umsetzbarkeit der Maßnahmen unter Einbeziehung interner und externer Ressourcen, wie etwa Managed Service Providern, gemeinsam sicherstellen,
- Rollen und Verantwortlichkeiten einschließlich Kommunikation unter Einbeziehung interner und externer Ressourcen, wie etwa Managed Service Providern, vollständig definieren und
- alle getroffenen Maßnahmen und Regelungen ausführlich dokumentieren.

Für einen adäquaten Schutz ist zu erörtern, welche Risiken es gibt, welche Bereiche besonders gefährdet sind und wie diese sich bestmöglich schützen lassen. So setzen Unternehmen die NIS-2 zuverlässig um.

Acuroc Solutions GmbH
Im Hostert 9
65510 Idstein
+49 (0) 6434 – 906 348
+49 (0) 6434 – 906 349
info@acuroc-solutions.de
www.acuroc-solutions.de